UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF A 2019 HONDA CIVIC WITH OHIO LICENSE PLATE KHE9672 AND VIN 2HGFC2F60KH536178	**CASE NO.** 2:25-mj-352 **MAGISTRATE JUDGE VASCURA** **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Tyler Schwab, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the search of the vehicle identified as a 2019 Honda Civic with Ohio License Plate KHE9672 and Vehicle Identification Number ("VIN") 2HGFC2F60KH536178 (the "SUBJECT VEHICLE"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 6, 2019. Your Affiant has been assigned to the FBI Safe Streets Task Force in Columbus, Ohio, since January of 2023. Prior to being assigned to the Safe Streets Task Force, I was assigned to the Joint Terrorism Task Force (JTTF) for approximately four years. During my assignment at the JTTF, I was a Case Agent and Co-Case Agent for multiple international and domestic terrorism investigations. While assigned to the JTTF, your Affiant received specialized training in international terrorism and homicide investigations. Furthermore, I have received training in computer-related crimes as well as in the criminal use of email, social media, and telephonic communications.

3. The facts in this affidavit come from information obtained from other law enforcement organizations to include the Columbus Police Department. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 2113(a) [bank robbery] and 18 U.S.C. § 924(c) [using a firearm during and in relation to a crime of violence] (the "Target Offenses") have been committed by JAMES TRAVIS SCURLOCK. There is also probable cause to search the SUBJECT VEHICLE, as described in Attachment A, for evidence, instrumentalities, contraband, and fruits of these crimes, as further described in Attachment B.

PROBABLE CAUSE

5. The United States, including the Federal Bureau of Investigation, is conducting a criminal investigation into violations of the Target Offenses. The current investigation involves a pair of bank robberies in which the subject entered the bank, pulled out what appears to be a handgun, and demanded cash. As of this writing of this affidavit, two bank robberies have occurred between March 6, 2025, and May 16, 2025, that are believed to have been committed by SCURLOCK.

Bank Robbery 1-Huntington Bank, 1146 Gemini Place, Columbus, Ohio 43240

6. On March 6, 2025, at approximately 12:38 p.m., Detectives with the Columbus Police Department responded to 1146 Gemini Place in reference to a bank robbery. Upon arrival, the detectives learned that a suspect had entered the Huntington Bank wearing a black zip-up hoodie, blue jeans, white Nike tennis shoes, black latex gloves, and a white camouflage mask.

7. The suspect approached a bank teller and asked about opening an account. When the bank teller asked the suspect if he had two forms of identification, the suspect stated that he did not. The bank teller then tried to schedule an appointment with the suspect later, when the suspect could come back with the proper identification. At that time, the suspect pulled out a black in color handgun, pointed it at the bank teller, and stated, "I'm sorry, I don't want to do this, don't do anything stupid. No dye packs. Give it all to me. No one move." The suspect was carrying a black Nike backpack with green piping and told the bank teller to place the money in the backpack. After the bank teller placed all the money in the drawer into the backpack, the suspect then directed the bank teller to another drawer and told the bank teller to empty that drawer as well. The bank teller ended up placing approximately $13,700 in cash into the suspect's backpack. The suspect then departed the bank. Moments after the suspect exited the bank, a red Honda Civic without a license plate can be seen on surveillance video exiting the bank parking lot.

8. Huntington Bank, whose deposits are federally insured, provided these photos of the suspect and what is believed to be the suspect's vehicle, which were both taken during the March 6, 2025 robbery:

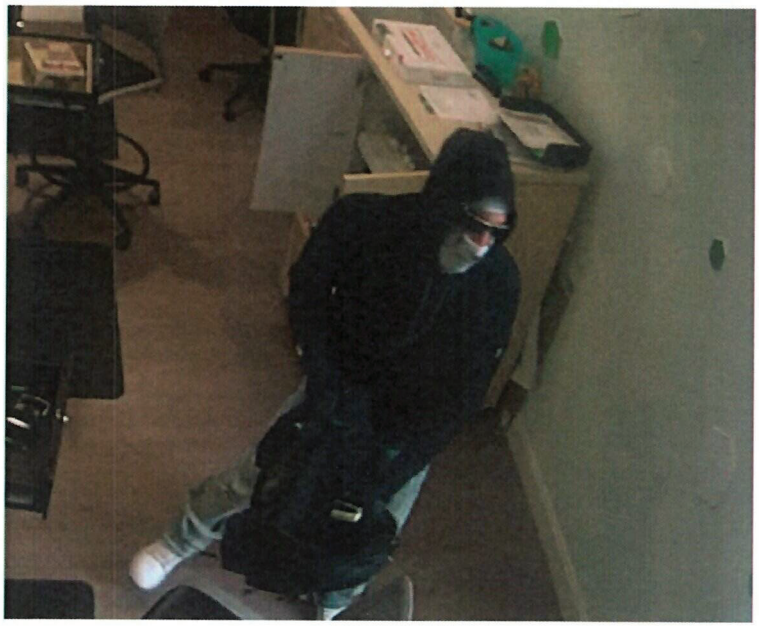
9. Todd Ballinger, Administrator with the Ohio Bureau of Motor Vehicles Investigation Section, was shown the above vehicle photo and identified the vehicle in the photo as a 2019 to 2022 Honda Civic.

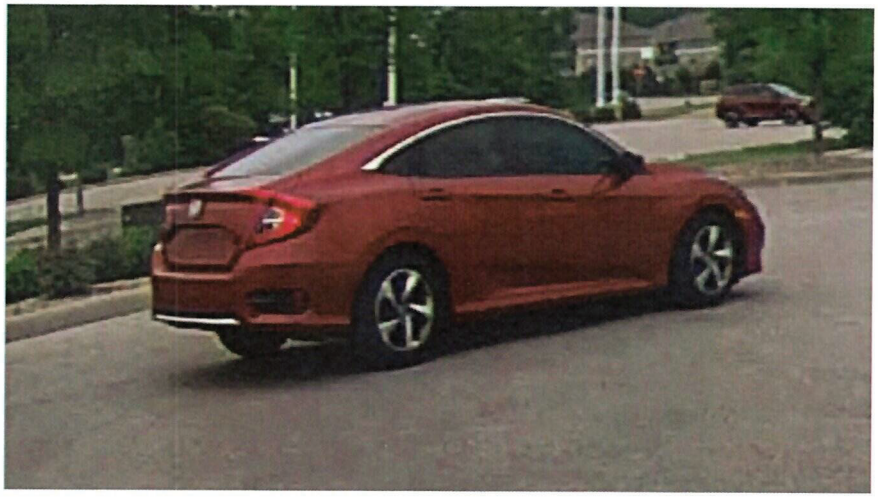
Bank Robbery 2-Huntington Bank, 1146 Gemini Place, Columbus, Ohio 43240

10. On May 16, 2025, at approximately 11:25 a.m., Detectives with the Columbus Police Department again responded to 1146 Gemini Place in reference to a bank robbery. Upon arrival, the detectives learned that a suspect entered the Huntington Bank wearing a black hoodie, blue jeans, white Nike shoes, black gloves, sunglasses, and a white camouflage mask.

11. Upon entering the bank, the suspect approached the teller and pulled out a black handgun. The suspect then said to the teller, "You know what to do," and "No dye packs." The suspect then walked to two tellers' drawers and placed the cash from their drawers into a black backpack. After doing this, the suspect then ordered the tellers to the vault and placed the cash from the vault into his backpack. The suspect then exited the bank. Shortly after the suspect exited the bank, a red Honda Civic without a license plate was seen exiting the parking lot. The suspect ended up getting away with a total of $27,715 from Bank Robbery 2.

12. Huntington Bank provided the following photos of the suspect and what is believed to be the suspect's vehicle, which were taken during the May 16, 2025, robbery:





13. It is the belief of the affiant that both robberies were committed by the same individual based on facts that the description and photos obtained of the potential suspect and his vehicle are similar in Bank Robbery 1 and Bank Robbery 2. In both bank robberies, the suspect wore a white camouflage mask, black hoodie, black gloves, blue jeans, white Nike shoes, and used a black backpack. Additionally, the vehicle that was seen departing the bank parking lot

after the suspect exited the bank in Bank Robbery 1 was a red Honda Civic without a license plate. This matches the description of the vehicle which was also seen departing the bank parking lot after the suspect exited the bank in Bank Robbery 2.

14. On March 14, 2025, United States Magistrate Judge Elizabeth A. Preston Deavers signed search warrants requiring AT&T and T-Mobile to provide the estimated location of all cellular devices that were within .35 miles of the Huntington Bank located at 1146 Gemini Place, Columbus, Ohio 43240, on the day (March 6, 2025) and during the time window (12:18 p.m. to 12:48 p.m.) of Bank Robbery 1. An analysis of the records provided by T-Mobile indicated that the cell phone associated with IMSI 310260492082206 was present at Bank Robbery 1 during the time that Bank Robbery 1 occurred.

15. Furthermore, grand jury subpoena returns from T-Mobile revealed that the phone number associated with IMSI 310260492082206 was (740) 972-5966 (the "TARGET CELL PHONE"). The same grand jury subpoena returns from T-Mobile revealed that the subscriber of the TARGET CELL PHONE was JAMES SCURLOCK.

16. Following Bank Robbery 2, Columbus Fire Department Investigator Jeremy Hinesman conducted a FLOCK camera search for red Honda Civics in the vicinity of the Huntington Bank located at 1146 Gemini Place, Columbus, Ohio 43240 between 10:00 a.m. and 1:00 p.m. on May 16, 2025. Investigator Hinesman observed a red Honda Civic on FLOCK camera at approximately 10:03 a.m. on May 16, 2025, driving on Old State Road at Powell Road, which is approximately 1.2 miles north of the Huntington Bank. The red Honda Civic on the FLOCK camera appeared similar to the red Honda Civic seen departing the bank shortly after the suspect exited the bank during Bank Robbery 1 and Bank Robbery 2. The license plate on the red Honda Civic, which was observed by Investigator Hinesman on FLOCK camera on May

16, 2025, had an Ohio license plate KHE9672. The red Honda Civic with Ohio license plate KHE9672 was found to be registered to SCURLOCK and was a 2019 model.

17. Based on the TARGET CELL PHONE, which is subscribed to SCURLOCK, being present at Bank Robbery 1, and SCURLOCK's registered red Honda Civic being in the area of Bank Robbery 2 prior to Bank Robbery 2 taking place, your affiant believes that SCURLOCK committed Bank Robbery 1 and Bank Robbery 2. In my training and experience, I know that individuals who commit bank robberies often commit more than one bank robbery and use similar tactics and techniques in their robberies. In this case, the suspect committed Bank Robbery 1 and Bank Robbery 2 by driving his red Honda Civic and seems to have taken the license plate off the vehicle before committing the bank robberies. The suspect also wore similar clothes in both bank robberies, which was a black hoodie/jacket, black gloves, blue jeans, white Nike shoes, and white camouflage mask. The suspect also used a black handgun and carried a black backpack to carry the cash he stole in both robberies. Additionally, the suspect specifically requested no dye packs be placed in the cash by the tellers in Bank Robbery 1 and Bank Robbery 2.

18. According to OHLEG, the address listed on SCURLOCK's Ohio driver's license is 400 Park Street, Apartment E6, Cardington, Ohio 43315 (in Morrow County, within the Southern District of Ohio). Additionally, SCURLOCK's listed address in Accurint is also 400 Park Street, Apartment E6, Cardington, Ohio 43315. On May 19, 2025, a Special Agent was conducting surveillance at the 400 Park Street, Apartment E6. During the surveillance, the Special Agent observed SCURLOCK return to his residence driving the red Honda Civic with Ohio license plate KHE9672. The Special Agent observed SCURLOCK park the red Honda Civic with Ohio license plate KHE9672 in the area of the residence, exit the vehicle, and then

enter 400 Park Street, Apartment E6. Additionally, on May 29, 2025, SCURLOCK was observed during surveillance exiting and reentering 400 East Park Street, Apartment E6, to retrieve a package from the front porch. SCURLOCK also recently purchased a Kawasaki Ninja 650 motorcycle. On May 29, 2025, SCURLOCK registered and titled this motorcycle with the Ohio Bureau of Motor Vehicles. On the motorcycle title and registration, SCURLOCK listed his address as 400 Park Street, Apartment E6, Cardington, Ohio 43315.

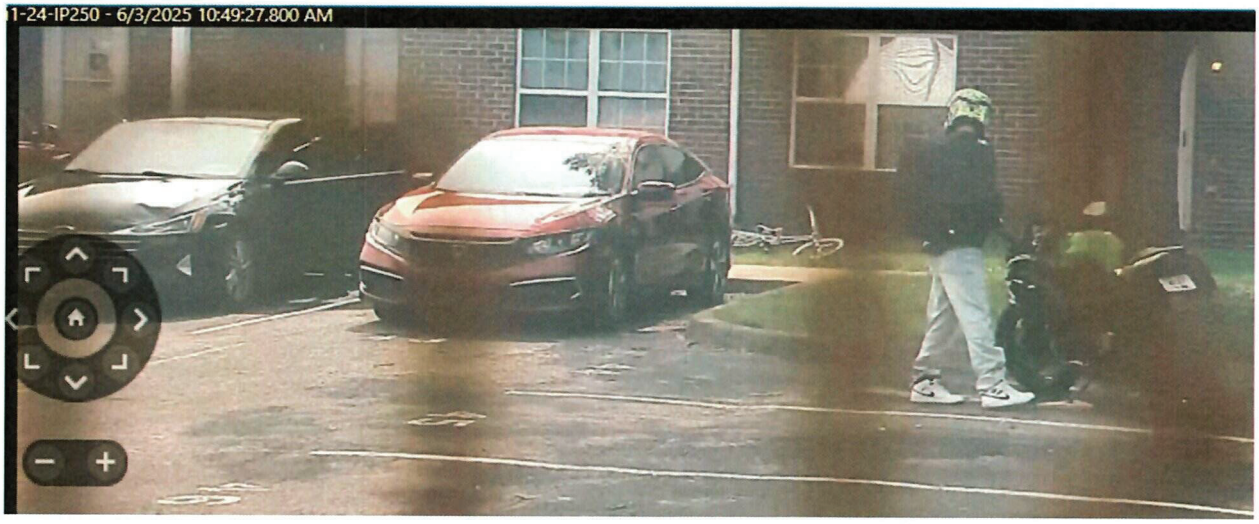
19. On May 20, 2025, United States Magistrate Judge Kimberly A. Jolson signed another search warrant, this one requiring T-Mobile to provide historical call detail records, including location information, for the TARGET CELL PHONE from March 1, 2025, to May 20, 2025 (location records ended up being from April 23, 2025, to May 20, 2025, based on T-Mobile's preservation of records policies). Analysis of the T-Mobile records shows that on the morning of May 16, 2025 (Bank Robbery 2), the TARGET CELL PHONE traveled from the area of the 400 Park Street, Apartment E6, to the Polaris Mall area. At approximately 10:17 a.m., the TARGET CELL PHONE was in the general area of Walmart located at 8659 Columbus Pike, Lewis Center, Ohio 43035, which was approximately 2.7 miles northwest of the Huntington Bank located at 1146 Gemini Place, Columbus, Ohio 43240 (location of Bank Robbery 1 and Bank Robbery 2). The TARGET CELL PHONE did not signal from 10:17 a.m. to 11:34 a.m. The timeframe that the TARGET CELL PHONE was not signaling encompassed the time that Robbery 2 took place, which was between 11:25 a.m. and 11:27 a.m. When the TARGET CELL PHONE next signaled, at 11:34 a.m., it was in the area of Interstate 71 and Alum Creek Lake. The TARGET CELL PHONE then regularly signaled to the area of the 400 Park Street, Apartment E6, and appeared to arrive at that location at approximately 12:02 p.m. There are several reasons why the TARGET CELL PHONE did not signal during the time of

Bank Robbery 2, one of them being that SCURLOCK could have turned off his phone. In my training and experience, I have learned that individuals who commit robberies often turn off their cell phones when they commit their robberies as a way to hide their location during the time of the robbery from law enforcement. In this case, SCURLOCK's phone was regularly signaling as he drove from Cardington to the Polaris Mall area on the morning of May 16, 2025. Once SCURLOCK got close to the site of Bank Robbery 2, he may have turned off his phone (approximately 10:17 a.m.). SCURLOCK may have turned his phone back on after he committed Bank Robbery 2 (11:34 a.m.), when he was out of the area of the bank robbery and was on Interstate 71 driving north toward his residence in Cardington, Ohio.

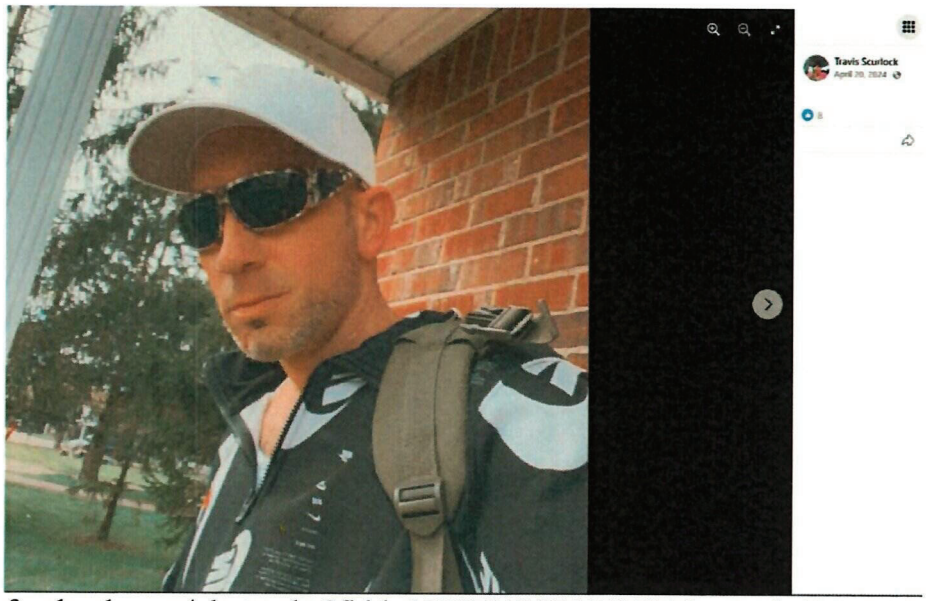
20. The call detail records and location information from T-Mobile also show that SCURLOCK frequents 400 Park Street, Apartment E6. The TARGET CELL PHONE repeatedly utilized cellular towers in the area of 400 Park Street, Apartment E6, including over extended hours of the day and at night. Additionally, a video surveillance vehicle was parked near 400 Park Street, Apartment E6 from June 2, 2025, to June 5, 2025. During that timeframe, the video surveillance vehicle captured footage of SCURLOCK regularly entering and exiting 400 Park Street, Apartment E6.

21. On June 3, 2025, at approximately 10:49 a.m., the video surveillance truck also captured SCURLOCK exiting 400 Park Street, Apartment E6, and getting on his Kawasaki Ninja 650 motorcycle. SCURLOCK can be seen wearing shoes that appear similar to the shoes that the suspect wore during Bank Robbery 1 and Bank Robbery 2. During those robberies, the suspect wore white Nike shoes with a black Nike swoosh on the outside and inside of each shoe. Before getting on the motorcycle, SCURLOCK can be seen wearing white Nike shoes with a black Nike Swoosh on the outside and inside of each shoe. Comparison photos taken from the

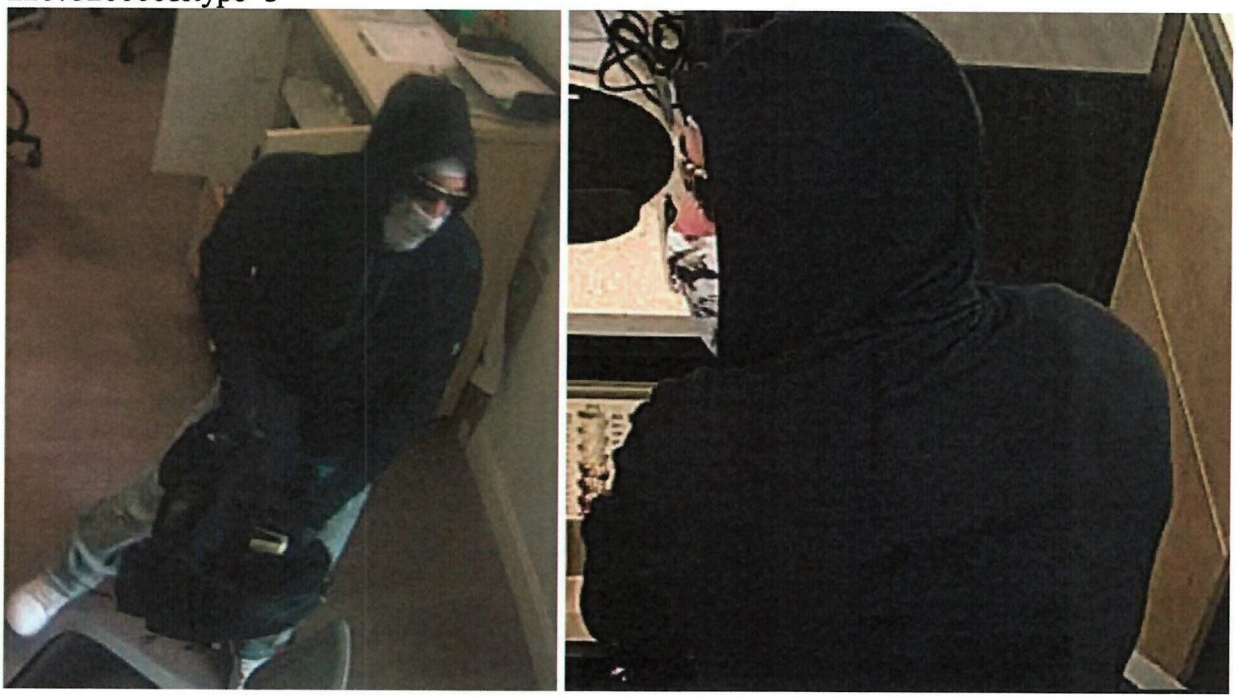
video surveillance vehicle on June 3, 2025, showing SCURLOCK near his motorcycle, and from the suspect during Bank Robbery 2, are shown below:



22. Investigators also looked at SCURLOCK's Facebook page, which uses the handle "Travis Scurlock." Your affiant knows that "Travis" is JAMES SCURLOCK's middle name. One of the photos posted on that account, with an apparent posting date of April 20, 2024, shows SCURLOCK wearing a pair of wrap-around camouflage sunglasses similar in appearance to the pair that the suspect wore during the commission of Bank Robbery 2. Comparison photos from SCURLOCK's Facebook account and Bank Robbery 2 are shown below:



https://www.facebook.com/photo.php?fbid=10227358876172581&set=pb.1081484762.-2207520000&type=3



23. Based on my training, experience, and participation in this investigation, I know that banks and financial institutions often organize cash using bands or straps, so that the cash can be counted easily. I also know that banks may store cash in bags or in plastic wrapping.

24. I know, based on my knowledge, training, and experience, that individuals who commit bank robberies often possess other items commonly used or acquired in connection with

those robberies. These items include, but are not limited to, firearms, firearm parts, ammunition, face masks, other disguises, and stolen cash. I also know based on my knowledge, training, and experience that individuals who are involved in the criminal activity described above often store those firearms, firearm parts, ammunition, face masks, other disguises, stolen cash, and the like within their homes, within their cars, and, in some instances, on their persons, so that those items are easily accessible. I also know that those items are all non-perishable goods, which can be expected to remain in the individual's possession for extended periods of time.

25. I also know that individuals who are involved in the criminal activity described above often use cell phones to coordinate, plan, execute, hide evidence, and avoid detection for such criminal activity. More specifically, I know that individuals involved in the criminal activity described above often use cell phones to coordinate meetups with co-conspirators and others involved in the planning and execution of the bank robberies. Those individuals also use cell phones for navigation purposes both to and from the site of a robbery. Likewise, those individuals may use cell phones to take photographs and videos of themselves in possession of stolen cash. The individuals may also use cell phones to destroy or hide evidence of their crimes, to discuss and/or divide the proceeds of their crimes, and to avoid detection for their crimes. This use of cell phones involves calls, texts, social media applications, navigation tools, and a host of other available applications. Indeed, the T-Mobile search warrant returns regarding Bank Robbery 1 showed that the TARGET CELL PHONE was signaling in the area of the Huntington Bank during the timeframe of that robbery.

26. I also know from my training and experience that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is

indispensable to participation in modern society." *Carpenter v. United States*, 585 U.S. 296, 315 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for records that might be found in the SUBJECT VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media (which includes a smartphone or cellular telephone). Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable Cause.* I submit that if a computer or storage medium is found in the SUBJECT VEHICLE, there is probable cause to believe those records will be stored on that computer or storage medium for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, it remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they

are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the Target Offenses, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic evidence will be on any storage medium in the SUBJECT VEHCILE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were

recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media

activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to facilitate the commission of a crime, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the site of a search, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used

for, and who has used it requires considerable time, and taking that much time on-site could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the

warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many partes of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. Based on the foregoing, probable cause exists to search the SUBJECT VEHICLE identified in Attachment A, for the items described in Attachment B and to seize those items.

Respectfully submitted,

Tyler Schwab
Special Agent
FBI

Subscribed and sworn to before me on June 9, 2025

HONORABLE CHELSEY M. VASCURA
UNITED STATES MAGISTRATE JUDGE